Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

NLIIBK14

2017

Sauli Alaranta

EU:N TIETOSUOJA-ASETUS - OIKEUS TULLA UNOHDETUKSI

– Case: Service Desk

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma | Tietoliikenne ja tietoturva

2017 | 43

Sauli Alaranta

EU:N TIETOSUOJA-ASETUS - OIKEUS TULLA UNOHDETUKSI

- Case: Service Desk

Tämän opinnäytetyö oli osana laajempaa projektia Turun ammattikorkeakoululle, joka haluaa tuoda tietosuoja käytäntönsä EU:n uuden tietosuoja-asetuksen 679/2016 mukaiseksi. Opinnäytetyön osuus projektista käsittelee oikeutta tulla unohdetuksi tietojärjestelmässä.

Teoriaosuudessa käytiin läpi opinnäytetyöhön liittyviä asioita. Nämä asiat käsittelevät tietosuojaa, henkilörekisteriä, Suomen lainsäädäntöä sekä EU:n uutta tietosuoja-asetusta. Näiden pohjalta pystyttiin kehittämään empiirisessä osiossa laadittu oikeus tulla unohdetuksi -artiklan selvitys. Toimeksiantaja pystyy käyttämään laadittua selvitystä hyväksi toimintatapojaan suunniteltaessa, tietosuojan kannalta. Tutkimuksessa selvinneitä kohtia hyödynnettiin toimeksiantajan käyttämään tietokantajärjestelmään, jotta rekisteröidyn oikeus tulla poistetuksi pystytään siinä toteuttamaan.

Henkilörekisterin tietojen poistamisen tavan ratkaisemiseksi, ideoitiin hypoteeseja, jotka voisivat toimia ratkaisuna tietojen säilyttämiseen ja poistamiseen. Mallit perustuivat toimeksiantajan antamiin tärkeimpiin vaatimuksiin tietojen poistamisen osalta, sekä uudesta tietosuoja-asetuksesta 679/2016 poimittuihin tietoihin. Ratkaisuja analysoitiin yhdessä toimeksiantajan kanssa, ja heille valittiin sopiva vaihtoehto käytännön testaamista varten. Tätä valittua ideaa kokeiltiin proof of concept -menetelmällä, tilaajan OTRS -järjestelmään, josta saatuja tuloksia toimeksiantaja pystyy hyödyntämään.

ASIASANAT:

yleinen tietosuoja-asetus, henkilötietorekisteri, henkilötietolaki, tikettijärjestelmä

BACHELOR´S / MASTER'S THESIS THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information technology

2017 | 43

Sauli Alaranta

GENERAL DATA PROTECTION REGULATION – RIGHT TO BE FORGOTTEN

- Case: Service Desk

The objective of this thesis was to be part of a greater project for Turku University of Applied Sciences. Their plan is to update their data protection principles to match European Union's General Data Protection Regulations 679/2016. Part of this thesis in the project consists article 17: Right to be Forgotten.

Theory section includes information of data protection, person register, Finnish law and EU GDPR. Knowledge gained from theory was used to form an interpretation of a right to be forgotten. The company can use this interpretation to form principles which are written in their data protection plans. Findings of interpretation were used to build a plan to delete personal data from person register, which can be executed in a system that they use.

Hypotheses to solve data storage and removal were planned together with the company. These hypotheses based on demands from company and EU GPDR. After reviewing each solution, decisions were made and anonymization was chosen to be used for more research. This plan was tested in a method of Proof of Concept and the test results can be used when decisions based on future of the existing system are made.

KEYWORDS:

general data protection regulation, person register, personal data law, ticketing system

SISÄLTÖ

KUVAT

KUVIOT

TAULUKOT

KÄYTETYT LYHENTEET JA TERMIT

Anonymisointi	Tiedon muokkaamista sellaiseksi, että sitä ei pystytä enää yhdistämään alkuperäiseen.
Asetus	Euroopan unionissa tehty päätös, joka tulee voimaan sellaisenaan jokaisessa jäsenvaltiossa. Asetus kumoaa kaikki sen kanssa ristiriidassa olevat kansalliset lait ja säädökset.
Artikla	Lain, kansainvälisen sopimuksen tai EU:n säädöksen osa, joka auttaa jäsentämään sen sisältöä. Suomen lainsäädännössä artiklaa vastaa *pykälä*.
Direktiivi	Euroopan unionin jäsenvaltioille annettu lainsäädäntöohje.
OTRS	Open-source Ticket Request System. Ilmainen ja avoimeen lähdekoodiin perustuva lupien pyytämisjärjestelmä.
Pseudonymisointi	Tietokokonaisuuden tunnistettavimpien arvojen muuttamista pseudonyymiksi eli alkuperäisestä irralliseksi. Tietoa pystytään yhdistämään suunniteltuja tunnisteita käyttäen.
SQL	Structured Query Language. Standardoitu kyselykieli, jolla tehdään relaatiotietokantaan erilaisia hakuja, muutoksia ja lisäyksiä.
Tiketti	Tikettijärjestelmien käyttämä nimitys lupapyynnöistä. Kutsutaan myös työpyynnöiksi.

1 JOHDANTO

Euroopan unionin säännökset tietosuojan osalta ovat uudistuneet. Tämän seurauksena sen jokaisen jäsenvaltion tulee päivittää lainsäädäntönsä vastaamaan uutta tietosuoja-asetusta 679/2016. Uudistuksen tarkoituksena on olla vahvistuksena säännöille, jotka suojelevat luonnollisten henkilöiden henkilötietojen käsittelyä. Tällaisia ovat heidän perusoikeutensa ja -vapautensa sekä erityisesti oikeus henkilötietosuojaan. (Tietosuoja-asetus 679/2016.)

Uudistuksen seurauksena henkilötietoja käsittelevien rekisterinpitäjien ja muidenkin henkilötietoja käsittelevien tahojen tulee tarkastella omaa toimintaansa ja tehdä muokkauksia toimintatapoihinsa sekä järjestelmiin. Niiden tulle olla asetuksen mukaisia, kun asetuksen siirtymäaika päättyy ja se siirtyy sovellettavaksi täysimääräisesti 5/2018 jälkeen. (Andreasson ym. 2015, 29.)

Koska Suomen nykyinen lainsäädäntö perustuu myös uuden asetuksen tavoin Euroopan unionin aiempaan tietosuojadirektiiviin 95/46/EY, on molemmissa hyvinkin paljon yhtäläisyyksiä. Uudistuksessa on kuitenkin huomattavasti yksityiskohtaisempia ja tarkempia määritelmiä tietojen säilytyksen osalta. Käytännössä tämä tarkoittaa aiempaa läpinäkyvämpää, lainmukaisempaa ja asianmukaisempaa tietojenkäsittelyä rekisterinpitäjältä rekisteröidylle. Asetuksen ollessa vain muutaman vuoden vanha, ei tietojen säilyttämisen ja poistamisen kannalta käytännön ratkaisun malleja ole juurikaan julkaistu. Kuitenkin itse tietosuoja-aiheesta löytyy hyvin paljon tietoa tietosuojavaltuutetun toimiston sivustolta sekä alan ammattilaisten julkaisuista, joissa tietojen säilyttämistä yleisesti käsitellään.

Tämän tutkimuksen tavoitteena oli selvittää millaisia vaatimuksia asetus tuo rekisterinpitäjälle tietojen säilyttämiseen ja poistamiseen liittyen. Tarkoitus oli tulkita asetusta ja luoda ratkaisumalli, jonka pohjalta olisi mahdollista olemassa olevan tietojärjestelmän uudistus toteuttaa. Tutkimus on tarpeellinen, sillä työn tilanneella Turun ammattikorkeakoululla oli edessä tilanne, jossa heidän tuli päivittää toimintansa tietosuoja-asetuksen 679/2016 mukaiseksi. Toimeksiantaja pyysi selvitystä etenkin asetuksessa mainitusta *oikeudesta tulla unohdetuksi* tietojärjestelmässä ja ratkaisuista, joilla se voidaan toteuttaa heidän järjestelmässään.

Opinnäytetyön teoriaosuudessa selvitettiin mitä tarkoittaa tietoturva ja siihen liittyvä tietosuoja, millaisia ovat henkilörekisterit sekä minkälaisia lakisäännöksiä niiden ylläpitämisellä on Suomessa. Teoria osuudessa perehdytään myös tietosuoja-asetukseen ja selvitetään, millä tavalla se käsittelee tietojen säilyttämistä.

Empiirisessä osuudessa tutkittiin mitä oikeus tulla unohdetuksi tarkoittaa, sekä minkälaisia toimia sen toteutuminen vaatii. Tämän lisäksi tutkittiin toimeksiantajan Service Desk -yksikön OTRS -tietojärjestelmän mahdollisuuksia, tietojenpoistamispyynnön osalta. Hypoteeseja tietojensäilyttämisen ja poistamisen ratkaisuiksi ideoitiin seitsemän kappaletta. Ne perustuivat EU:n tietosuoja-asetukseen 679/2016 ja aikaisempiin käyttäjäkokemuksiin kyseisestä järjestelmästä. Hypoteesit liittyivät tiedon arkistoinnin, poistamisen, pseudonymisoinnin ja anonymisoinnin menetelmiin.

Toimeksiantaja valitsi ideoiduista ratkaisuista anonymisoinnin, jota kokeiltiin käytännössä Proof of Concept -menetelmällä. Anonymisointi tietojen säilytyksen ratkaisuna todettiin yleisesti toimivaksi menetelmäksi henkilötietojen poistamiselle, mutta järjestelmän valmistajakohtaiset ratkaisut tuottivat haasteita käytännön toteutukselle, esimerkiksi asiakastietojen poistamiselle palvelimelta.

2 TIETOTURVAN PERUSTEET

Tietoturvallisuus on hyvin olennainen osa rekisterinpitäjän velvollisuuksia, tämän vuoksi on tarpeellista ymmärtää mitä tietoturvalla tarkoitetaan. Suurin osa ihmisistä varmasti ymmärtää tietoturva-termin käsitteenä tietojen suojaamiselle negatiivisilta asioilta. Ammattikielessä tietoturva-terminä on kuitenkin vain yksi osa sitä kokonaisuutta, joiden tarkoituksena on turvata tietoja kaikelta mahdolliselta uhalta. Tämä tarkoittaa sitä, että suojaamista lähestytään kolmelta eri aspektilta, jotka ovat tietoturvallisuus, tietoturva ja tietosuoja. Nämä kolme termiä käsittävät jokainen oman alueensa, joista sitten muodostuu kokonaiskuva siitä tietojen suojaamisesta, jota käytetään onnistuneen tietoturvan muodostamiseen. (Laakso 2013, 5.)

2.1 Tietoturva

Tietoturva on hyvinkin moniulotteinen asia. Riippuu pitkälti tahosta, kuinka he sen käsittävät. IT-asiantuntijat saattavat tarkoittaa teknistä näkökulmaa, mutta tietoturvavastaava saattaa nähdä asian enemmänkin hallinnollisena. Yleisesti ymmärrettynä tietoturva kuitenkin tarkoittaa tiedon ominaisuuksia. (Laakso 2013, 5–6.)

Ominaisuudet ovat alun perin pohjautuneet klassiseen tiedon määritelmään. Määritelmään kuuluu luottamuksellisuus, käytettävyys ja eheys. Kuitenkin tätä määrittelyä pidetään nykyaikana riittämättömänä, sillä niissä ei oteta huomioon itse laitteistojen tai tietoja tietoliikennejärjestelmien arvoa. Yleisin uusi laajennettu määritelmä käsittää vielä lisäksi kiistämättömyyden ja pääsynvalvonnan. (Hakala ym. 2006, 4.) Lisäksi joissakin alan esityksissä on sisällytetty määritelmä kuudennesta osa-alueesta eli autentikoinnista.

2.1.1 Luottamuksellisuus

Luottamuksellisuudella (confidentiality) tarkoitetaan, että ainoastaan asiaankuuluvilla henkilöillä on mahdollisuus päästä tietoihin sekä niitä käyttäviin järjestelmiin käsiksi. Tietoa ei saa paljastaa luvattomille. Luottamuksellisuuden säilymisen pysymiseksi käytetään mm. salaustekniikoita. (Hakala ym. 2006, 4.)

2.1.2 Pääsynvalvonta

Pääsynvalvonnalla (access control) tarkoitetaan niitä tapoja, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Tällöin pyritään estämään ulkopuolisia ja omia työntekijöitä käyttämästä organisaation laitteistoa sekä yhteyksiä omiin tarkoituksiinsa. Luvattomat käyttäjät kuormittavat laitteistoja sekä yhteyksiä ja altistavat tietojärjestelmät haittaohjelmille. Pääsynvalvonnan työvälineinä käytetään salasanoja, varmenteita, kuluntunnisteita sekä lokeja. (Hakala ym. 2006, 5-6.)

2.1.3 Eheys

Eheydellä (integrity) tarkoitetaan sitä, että olemassa olevat tiedot ovat loogisesti oikein. Tällöin niitä ei tule pystyä muokkaamaan asiattomasti tallennuksen ja tiedonsiirron aikana. Eheyden varmistumisen työvälineinä käytetään mm. tarkistussummia sekä tiivisteitä. (Hakala ym. 2006, 4.)

2.1.4 Kiistämättömyys

Kiistämättömyydellä (non-repudiation, accountability) tarkoitetaan sitä, että kaikesta tehdyistä toimenpiteistä jää järjestelmään todistettava jälki. Tällä pystytään yksilöimään tekijä juridisesti sitovalla tavalla ja tekijä ei tätä pysty kiistämään. Kiistämättömyyden seurantaan käytetään esimerkiksi lokeja ja autentikaatiota. (Hakala ym. 2006, 5.)

2.1.5 Käytettävyys

Käytettävyydellä (availability, accessibility) eli saatavuudella tarkoitetaan sitä, että palvelut, tiedot ja tietojärjestelmät ovat saatavilla ja käytettävissä aina silloin, kun niitä tarvitaan. Tiedot eivät saa vahingoittua tai hävitä itsekseen. Tiedoille ei saa tapahtua myöskään mitään tietoisen hyökkäyksen (hakkerien, viruksien) seurauksena. Työvälineitä käytettävyyden suojaamiselle on mm. tekniset järjestelyt, varmuuskopiot sekä suojausohjelmistot. (Hakala ym. 2006, 4.)

2.1.6 Autentikointi

Autentikoinnilla (authentication) tarkoitetaan sitä, että jokainen käyttäjä tunnistetaan luotettavasti sekä turvallisesti. Tällä voidaan varmentaa se, ettei yksikään käyttäjä pysty esiintymään toisena henkilönä. Autentikoinnin työvälineinä käytetään salasanoja sekä varmenteita. (Hakala ym. 2006, 6.)

2.2 Tietoturvallisuus

Tietoturvallisuus-terminä yhdistetään joskus rinnakkain tietoturvan kanssa, nämä kuitenkaan eivät tarkoita täysin samaa asiaa. Tietoturva keskittyy olennaisesti tiedon ominaisuuksien turvaamiseen, kun taas tietoturvallisuus tarkoittaa hallinnollisia järjestelyjä esimerkiksi lainsäädäntöön ja yrityksen tietoturvallisuuden tahtotilaan perustuen, joilla pyritään saavuttamaan tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvallisuus on enemmänkin kuin suuri kokonaisuus ja se jaetaan pienempiin osa-alueisiin, jotta sen hallitseminen olisi helposti lähestyttävää. Osa-alueet jaotellaan karkeasti hallinnolliseen, tekniseen ja henkilöstöön. On olemassa myös yksityiskohtaisempia luokitteluja. Tällainen on esimerkiksi Viestintäviraston jaottelu, johon kuuluvat hallinnollinen tietoturvallisuus, fyysinen turvallisuus, henkilöstöturvallisuus, tietoliikenne-, laitteisto- ja ohjelmistoturvallisuus sekä tietoaineisto- ja käyttöturvallisuus. (Laakso 2013, 5-6.)

2.3 Tietosuoja

Tietosuojalla (data protection) tarkoitetaan kansainvälisesti vakiintunutta termiä tarkoitettaessa henkilötietojen suojaa oikeuden määrittämin säädöksin. Tietosuoja itse käsitteenä johtaa hieman harhaan, eikä se tarkoita tietosuojan kohteena olevan turvaamista, vaan sen tarkoitus on olla keinona henkilötietojen suojaamiseksi (Koskinen ym. 2005, 49-50.)

Kunkin valtion voimassa olevin säädöksin, henkilötietojen suojaksi on säädetty henkilötietolaki, jonka tarkoitus on turvata yksityisten henkilöiden yksityisyys, oikeudet ja oikeusturva. Edellä mainitut kohdat tulee tulla varmistetuiksi heidän tietojansa kerätessä, käsiteltäessä ja säilyttäessä. (Opitietosuojaa.fi 2016).

Suomen laki ei ole määritellyt erikseen yksityisyyttä ja tietosuojaa. Tietosuoja-termi on kuitenkin ollut käytössä Suomen lainsäädännössä pitkän aikaa, koskien henkilörekisterilakia vuodelta 1988 sekä myöhemmin henkilötietolakia vuodelta 1999. Tällöin se on säännöksissä tarkoittanut henkilötietojenkäsittelyyn liittyviä velvollisuuksia ja oikeuksia. Tietosuojan merkitystä korostaa osaltaan se, että sitä ympäröi laaja erityislakien ja säädösten määrä, jotka ovat astuneet voimaan vuoden 1988 henkilörekisterilain hyväksymisen jälkeen. (Koskinen ym. 2005, 49.)

3 HENKILÖREKISTERI

Opinnäytetyön keskittyminen juuri henkilörekisterin ylläpitäjän velvollisuuksiin on relevanttia, että tiedetään mitä tarkoittaa on henkilörekisteri ja minkälaisen laillisen pohjan päälle se on rakennettu, Suomen lain säätämän vuoden 1999 henkilötietolain mukaan. Tietosuoja-asetusta ymmärtääkseen ja sitä soveltaessa olemassa olevaan asiakasrekisteriin on hyvä pystyä tunnistamaan nuo kohdat, joihin tulee kiinnittää huomiota. Nykyinen henkilötietolaki sisältää jo joitakin tulevan asetuksen mukaisia vaatimuksia.

3.1 Yleistä

Yritysmaailmassa on tarpeellista kerätä tietoa asiakkaista, jotta liiketoimintaa voidaan toteuttaa ja kehittää. Tämän vuoksi on tarkoituksenmukaista järjestää tiedot rekisteriin. Henkilötietorekisteri on tietopankki, ja se sisältää kaiken tärkeän ja tarvittavan tiedon asiakkaista. Rekisteri on keskeinen osa tätä järjestelmää, ja sen ympärille yleensä rakennetaan eri tiedonhallintasovelluksia. Tällöin organisaation eri osat pystyvät noutamaan tarvittavan asiakastiedon rekisteristä omaan tietojenkäsittelyynsä ja hyödyntämään tätä. (Rope & Pöllänen 1998, 113.) Rekisteri voi olla sekä manuaalisesti tai automaattisen tietojenkäsittelyn avustuksella hallittu järjestelmä tai sellainen, jossa tietoja käsitellään molemmin tavoin (Raatikainen 2000, 42).

Rekistereitä pidetään hyvin moneen eri tarkoitukseen. Monelle tuttuja ovat nykypäivänä yleistyneet, ihmisten ostokulttuurin ympärillä pyörivät markkinointiin tarkoitetut rekisterit, jotka keräävät tietoja asiakkaista ja kohdentavat näitä tietoja hyödyntämällä markkinointia räätälöidysti asiakkaillensa. Toisenlaisia rekistereitä ovat esimerkiksi yrityksen sisäiset palvelujärjestelmät, joissa välitetään työtikettejä työntekijältä toiselle ja näitä tikettejä täydennetään rekistereistä löytyvillä tiedoilla automaattisesti.

Asiakkaista kerättävä tieto jaetaan viiteen eri perusluokkaan: yhteystiedot, segmentointitiedot, käyttö- ja kokemustiedot, infotiedot sekä tulostiedot. Ne poikkeavat toisistaan tietojen hyödyntämisen näkökulmasta. On oleellista rekisterin toiminnan osalta, että edellä mainitut tiedot ovat jatkuvasti oikeellisia ja ajan tasalla, jotta niitä pystytään käyttämään sekä asiakasta ja yritystä, hyödyttävällä tavalla (Rope & Pöllänen 1998, 113-114.)

3.2 Suomen lainsäädäntö

Suomessa toimivalla taholla, joka ylläpitää tai käyttää henkilötietoihin perustuvaa rekisteriä on oltava tuntemus senhetkisestä lainsäädännöstä, joka määrittelee käsitteet henkilötietojen käsittelylle (Raatikainen 2000, 36). Tällä hetkellä Suomessa käytössä on vielä henkilötietolaki, joka on astunut voimaan vuonna 1999. Toukokuussa 2016 on kuitenkin otettu käyttöön siirtymävaihe uudistuneeseen Euroopan unionin yhteiseen tietosuoja-asetukseen 2016/679, jota sovelletaan täysimääräisesti toukokuun 2018 jälkeen (Euroopan parlamentin ja neuvoston asetus 2016/679). Tämä johtaa Suomen tietosuojaa koskevan lain päivittämiseen uudistuneen asetuksen mukaiseksi.

3.3 Henkilötietolaki

Suomen nykyinen lainsäädäntö perustuu Euroopan parlamentin ja neuvoston direktiiviin 95/46/EY, joka koskee yksilöiden suojelusta henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta. (Euroopan parlamentin ja neuvoston direktiivi 95/46/EY). Tämän asetuksen johdosta säädettiin henkilötietolaki 523/1999, joka kumosi aikaisemman henkilörekisterilain 481/1987. Henkilötietolain tehtävä on olla keinona suojaamassa yksityiselämää sekä olla osana edistämässä hyvän tietojenkäsittelytavan kehitystä ja noudattamista (Henkilötietolaki 523/99.)

Henkilötietolakia sovelletaan nimenomaisesti henkilötietojen käsittelyyn. Lain piirin kuuluvat sekä viranomaiset, yritykset, järjestöt, muiden yhteisöjen sekä yksityisten henkilöiden toimet. Loput toimijat, jotka jäävät soveltamisen ulkopuolelle käsittävät henkilökohtaisessa tarkoituksessa tapahtuvan tietojenkäsittelyn sekä tietyin rajoituksin henkilötietojenkäsittelyn toimituksellisia, taiteellisia ja kirjallisen ilmaisun tarkoituksia varten. Lakia sovelletaan sekä manuaaliseen, että automaattiseen tietojenkäsittelyyn henkilötietojen osalta, jotka ovat määritelty lain 3. pykälässä. (Henkilötietolaki 523/99.)

Laissa tarkoitetut määritelmät ovat seuraavat (Henkilötietolaki 523/99, 3. §):

1) *Henkilötiedolla* tarkoitetaan merkintää, jotka yhdistetään luonnolliseen henkilöön. Tällaisia ovat esimerkiksi hänen ominaisuudet, elinolosuhteita kuvaavat merkinnät, jotka voidaan tunnistaa hänen perhettään tai samassa taloudessa asuvia koskeviksi;

2) *henkilötietojen käsittelyllä* tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä;
3) *henkilörekisterillä* tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta;
4) *rekisterinpitäjällä* tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty;
5) *rekisteröidyllä* tarkoitetaan henkilöä, jota henkilötieto koskee;
6) *sivullisella* tarkoitetaan muuta henkilöä, yhteisöä, laitosta tai säätiötä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää;
7) *suostumuksella* tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

3.3.1 Periaatteet

Seuraavassa on koottu kohtia, jotka koskevat rekisterinpitäjää.

Rekisteripitäjän pääperiaatteisiin kuuluu henkilötietojen käsittely *laillisesti*, *huolellisuuden* noudattaminen ja *hyvän tietojenkäsittelytavan* käyttäminen. Tarkoituksena on, ettei rekisteröidyn oikeuksia rajoiteta ilman säädettyä perustetta. Tietojen käyttämisen tulee myös olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Myöhempää tietojen käyttämistä aikaisemmin perusteltujen tietojen vastaisesti ei pidetä sallittuna. Kuitenkin tästä on poikkeuksena historiallinen, tieteellinen ja tilastollinen tietojenkäsittely tarkoitus. (Henkilötietolaki 523/99, 5–7 §.)

Tietoja käsiteltäessä, niiden tulee täyttää *tarpeellisuusvaatimus* eli käytettävien tietojen tulee olla määritellyn käsittelyn mukaisia. Tämän lisäksi rekisterinpitäjän tulee huolehtia,

että tiedot täyttävät *virheettömyysvaatimuksen* eli tiedot eivät ole vanhentuneita, vääriä tai epätäydellisiä. (Henkilötietolaki 523/99, 9 §.)

Laissa määritellään arkaluontoisten henkilötietojen käsittelykiellosta, joka estää rotua tai etnistä alkuperää, yhteiskunnallista, poliittista, uskonnollista, ammattiliittoon, rikollista, terveyttä, seksuaalisuutta ja sosiaalihuoltoa koskevan tiedonkäsittelyn. Kuitenkin näissä kohdissa voidaan tehdä poikkeus sellaista syistä, jotka koskevat laillista velvoitetta, rekisteröidyn tai toisen henkilön elintärkeän edun suojaamiseksi, rekisteröidyn oman suostumuksen luvalla tai tietojen käsittelyyn historiallisessa, tieteellisessä tai tilastollisessa tarkoituksessa. Henkilötunnusta ei myöskään saa käsitellä ilman rekisteröidyn lupaa ja tälle käsittelylle on oltava laillinen perusta. (Henkilötietolaki 523/99, 11-13§.)

3.3.2 Rekisteröidyn oikeudet

Henkilötietolaki määrittää rekisteröidylle keinoja, joiden avulla hän pystyy kontrolloimaan luovuttamiensa tietojen käyttöä. Rekisterinpitäjällä on velvollisuus toimittaa tiedot rekisteröidylle rekisterinpitäjästä, tämän edustajasta ja henkilötietojen käsittelyn tarkoituksesta. Lisäksi tulee toimittaa tieto siitä mihin tietoja luovutetaan, ja selvitys siitä, kun tiedot on saatu muulta osapuolelta, kuin itse rekisteröidyltä. Näistä tulee välittää ilmoitus viimeistään silloin kun tietoja käsitellään. (Henkilötietolaki 523/99, 24§.)

Rekisteröidyllä on myös tarkastusoikeus tietoihinsa, jolloin rekisteröidyllä on oikeus saada tietää, käsitelläänkö hänen tietojaan ja sisältääkö rekisteri hänen tietojaan. Tarkastusoikeus ei kuitenkaan toteudu, jos se liittyy valtion turvallisuuteen, rikoksien ehkäisemiseen tai aiheuttaa vaaraa rekisteröidylle taikka muille. Lisäksi tarkastusoikeus ei toteudu, jos käsittely liittyy valvonta ja tarkastustehtäviin Suomen ja EU:n taloudellisen edun vuoksi tai historiallisen, tieteellisen taikka tilastollisen tutkimuksen vuoksi. Tätä oikeutta varten on rekisteröidyn itse toimitettava laillinen todiste tietojen pyytämisestä rekisterinpitäjälle. Tällöin rekisterinpitäjän on ilman aiheetonta viivästystä tarjottava rekisteröidylle mahdollisuus pyydettyihin tietoihin. (Henkilötietolaki 523/99, 26–28 §.)

Rekisterinpitäjän on ilman aiheetonta viivästystä oma-aloitteisesti tai rekisteröidyn pyynnöstä poistettava, oikaistava tai täydennettävä rekisterissä säilytettävä tieto, joka on käsittelyn kannalta puutteellinen, vanhentunut, tarpeeton tai virheellinen. Tällaisen tiedon leviäminen on myös estettävä rekisterinpitäjän toimesta, jos se vaarantaa rekisteröidyn

suojaa ja oikeuksia. Rekisteröidyllä on myös oikeus kieltää rekisterinpitäjää käsittelemästä häntä koskevia tietoja suoramarkkinointia, etämyyntiä sekä markkina -ja mielipidetutkimusta, kuten myös henkilömatrikkelia ja sukututkimusta varten. (Henkilötietolaki 523/99, 29-30§.)

3.3.3 Tietojensäilytys

Henkilötietolaki määrittelee henkilötietoja käsitteleville tahoille määräyksiä ja velvollisuuksia tietojen säilyttämistä koskien. Rekisteröidyn on toteutettava kaikki tarpeelliset tekniset ja organisatoriset toimenpiteet, jotta henkilötiedot suojataan asiattomilta pääsyiltä tietoihin ja vahingossa tai laittomasti tapahtuvan tietojen häviämisen, muuttumisen, luovuttamisen, siirtämisen taikka muun laittoman käsittelyn vaaroilta. Toteutettavien toimenpiteiden käyttämisessä tulee ottaa huomioon tekniset mahdollisuudet, kustannukset, tietojen laatu, määrä, ikä sekä käsittelyn merkitys. (Henkilötietolaki 523/99, 32 §.)

Henkilörekisteri, joka ei enää täytä tarpeellisuusvaatimuksia rekisterinpitäjän toiminnan kannalta, tulee hävittää. Tähän sallitaan poikkeuksia, jos tiedot ovat erikseen määrätty säilytettäväksi tai ne siirretään arkistoon. Arkistointiin tarkoitettuun tietoon tulee soveltaa sen hetkisiä säädöksiä. Tulee myös ottaa huomioon henkilötietojen käsittelystä ja luovuttamisesta säädettyä lakia, ellei se tietojen laadun ja iän huomioon ottaen ole tarpeetonta. (Henkilötietolaki 523/99, 34-35 §.)

4 EU:N TIETOSUOJA-ASETUS

Euroopan unioni on päättänyt päivittää tietosuojasäädäntöjään. Päätöksen johdosta voimaan on astunut uusi yleinen tietosuoja-asetus alkaen 24. toukokuuta 2016, jonka tarkoituksena on korvata vanha 95/46/EY direktiivi. Uuden asetuksen voimaan astuessa on alkanut kahden vuoden siirtymäaika, jonka aikana sovelletaan näitä asetuksia. Siirtymäajan loputtua 25. toukokuuta 2018 on kunkin rekisteröidyn jäsenvaltion henkilötietojen käsittelyn oltava uuden EU tietosuoja-asetuksen mukaisia. (Tietosuojavaltuutetun toimisto 2017.)

Yleisen tietosuoja-asetuksen tarkoituksena on tuoda tietosuojaa koskeva sääntely nykypäivän vaatimuksien tasolle, jotta voidaan vastata nykyteknologian ja globalisaation henkilötietojen suojaa koskeviin haasteisiin. EU jäsenmaiden välillä on myös ollut tähän asti hyvin vaihtele taso tietosuojaan liittyen. Asetuksien on tarkoitus nyt yhtenäistää jokaisen jäsenvaltion tietosuojaa koskevat säännökset, jotka osaltaan rakentavat yhtenäisyyttä ja luottamusta. Tämän toivotaan vaikuttavan esimerkiksi digitaalitalouden positiiviseen kehitykseen sisämarkkinoiden alueella. Tarkoituksena on myös sujuvoittaa henkilötietojen liikuteltavuutta kansainvälisesti. Käytännön tasolla tietosuoja-asetuksen on tarkoitus lisätä avoimuutta ja läpinäkyvyyttä henkilötietoja käsiteltäessä sekä vahvistaa jokaisen rekisteröidyn oikeutta valvoa näiden käsittelyä. (Tietosuojavaltuutetun toimisto 2017.)

Asetuksen velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla. Asetuksessa on säädetty Suomen nykyistä henkilötietolakia tiukemmat seuraamukset toimista, jotka ovat asetuksen vastaisia. Valvontaviranomainen voi tällöin esimerkiksi määrätä henkilötietojen käsittelyyn liittyviä korjaavia toimenpiteitä tai jopa hallinnollisia sakkoja. (Tietosuojavaltuutetun toimisto 2017.)

EU tietosuoja-asetus koskee jokaista sen soveltamisalaan kuuluvaa henkilötietojen käsittelyyn liittyvää organisaatiota, niin henkilötietojen käsittelijöitä kuin rekisterinpitäjiä. Asetuksen soveltamisalaa rajaavat sen alueellista ja aineellista soveltamisalaa koskevat säännökset. Joissain tietyissä asetuksissa sitä sovelletaan myös EU:n ulkopuolelle sijoittuneihin organisaatioihin. Asetus on sovellettuna sekä yksityisellä että julkisella sektorilla yhtenäisesti, eikä sillä ole eroa kuinka laajasti tietoja käsitellään, minkä luontoisia henkilötiedot ovat tai millaista teknologiaa niiden käsittelyssä käytetään. Asetusta sovelletaan automaattiseen henkilötietojen käsittelyyn sekä silloin kun henkilötiedot muodostavat rekisterin osan. (Tietosuoja-asetus 679/2016, 2-3 artikla.)

4.1 Määritelmä

Tietosuoja-asetuksessa henkilötiedon käsiteet on määritelty lähes vastaavalla tavalla kuin nykyisessä Suomen henkilötietolaissa 523/1999. Kuitenkin asetuksessa määritelmä on henkilötietolakia hieman yksityiskohtaisempi ja sen sisällössä on konkreettisia esimerkkejä henkilötiedoiksi määriteltävistä tiedoista. Lisäksi määritelmiin on lisätty mm. seuraavat kohdat (Tietosuoja-asetus 679/2016, 3 artikla.):

1) *Käsittelyn rajoittaminen,* jolla rajoitetaan henkilötietojen myöhempää käyttämistä.
2) *profilointi*, jolla automaattisesti arvioidaan henkilön tiettyjä henkilökohtaisia ominaisuuksia.
3) *pseudonymisointi,* jolla henkilötietoja käsitellään niin, ettei niistä ole enää henkilöä tunnistettavissa ilman lisätietoja. Lisätiedot säilytetään erillään teknisiä ja organisatorisia toimenpiteitä käyttäen.
4) *kolmas osapuoli,* tarkoittaa osapuolta, jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai käsittelijän välittömän vastuun alaisena.
5) *henkilötietojen tietoturvaloukkauksella,* jolla tarkoitetaan henkilötietojen vahingossa tapahtuvaa tai lainvastaista tuhoutumista, häviämistä, muuttamista, luvatonta luovuttamista tai pääsyä tietoihin.

4.2 Periaatteet

Asetuksen 5. artiklassa käydään läpi henkilötietojen käsittelyä koskevat periaatteet. Lähtökohtana on, että henkilötietoja tulee käsitellä lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. Henkilötietoja tulee kerätä vain tiettyä tarkoitusta varten, joka on nimenomainen sekä laillinen. Näitä tietoja ei saa käsitellä myöhemmässä vaiheessa alkuperäisen keräys tarkoituksen vastaisesti. Henkilötietojen on myös oltava asianmukaisia, olennaisia sekä niiden määrää tulee rajoittaa mahdollisimman vähään. Tämän lisäksi käsiteltävien tietojen on oltava jatkuvasti täsmällisiä ja päivitettyjä sekä rekisterinpitäjän on tehtävä kaikki mahdollinen, jotta käsittelyssä olevat virheelliset henkilötiedot saadaan oikaistua tai poistettua. Henkilötietoja tulee myöskin säilyttää sellaisessa muodossa, josta rekisteröity voidaan tunnistaa ainoastaan niin kauan, kuin se on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. (Yleinen tietosuoja-asetus 2016, 5 artikla.)

Henkilötietoja voidaan kuitenkin säilyttää pidempiä aikoja, jos niitä käsitellään ainoastaan tilastollisia, tieteellisiä tai historiantutkimus tarkoituksia varten, jotka ovat artiklan 83 vahvistettujen sääntöjen sekä edellytysten mukaisia. Tällöin tietojen säilyttämisen tarpeellisuutta tulee arvioida säännöllisesti uudelleen. (Yleinen tietosuoja-asetus 2016, 5 artikla.)

Asetuksen 6. artikla perehtyy henkilötietojen käsittelyn lainmukaisuuteen. Käsittely on lain mukaista ainoastaan silloin, kuin se täyttää vähintään yhden asetetuista edellytyksistä. Edellytykset käsittävät tällaisia kohtia, kuten henkilö on itse antanut suostumuksen tietojen keräämiseen, henkilö on osana sellaista sopimusta, joka edellyttää tietojen käsittelyä tai käsittely olisi tarpeen sellaisessa tilanteessa, jossa suojataan rekisteröidyn elintärkeitä etuja. Tietojen käsittelijä on velvollinen käsittelemään tietoja lakisääteisten velvoitteiden noudattamisen vuoksi tai rekisterinpitäjällä on tarve käsitellä tietoja oikeutetun etunsa nimissä. Henkilötietojen käsittely on myös laillista historiantutkimuksessa, tilastollisessa tai tieteellisissä tutkimuksissa, kunhan ne täyttävät artiklan 83 vaatimukset. Kunkin jäsenvaltion on säädettävä lakinsa noudattamaan edellä mainittuja säädöksiä, joita sovelletaan sitten rekisterinpitäjiin. (Yleinen tietosuoja-asetus 2016, 6 artikla.)

Seitsemännessä artiklassa käydään läpi suostumuksen edellytyksiä. Rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut oman suostumuksensa tiettyjen tarkoituksien mukaista käsittelyä varten. Kirjallisissa suostumustilanteissa on vaatimuksen oltava selvästi myös erillään muista asioista epäselvyyksien poistamiseksi. Rekisteröidyllä tulee olla oikeus peruuttaa suostumuksensa, milloin tahansa. Myöskään suostumus ei anna henkilötietojen käsittelylle oikeusperustaa, jos rekisteröidyn ja rekisterinpitäjän välillä on selviä merkkejä epäselvyydestä. (Yleinen tietosuoja-asetus 2016, 7 artikla.)

Artikla 8. sen sijaan käsittelee erikseen lapsen oikeuksia henkilötietojen käsittely tilanteessa. Alle 13-vuotiaan lapsen tietojen käsittely on lainvoimaista ainoastaan sellaisessa tilanteessa, jossa lapsen vanhempi tai huoltaja on siihen antanut suostumuksen tai valtuutuksen. Rekisterinpitäjän on käytettävä kohtuullisia toimenpiteitä, jotta tämä suostumus voidaan todentaa oikeaksi. (Yleinen tietosuoja-asetus 2016, 8 artikla.)

Yhdeksäs artikla määrittelee erityisiä tietoryhmiä koskevasta käsittelystä. Siinä kielletään sellaisten henkilötietojen käsittely, jotka koskevat rotua tai etnistä alkuperää, poliittista mielipidettä, uskonnollista tai filosofista vakaumusta, ammattiliittoon kuulumista, geneet-

tistä tai seksuaalista käyttäytymistä, rikostuomiota tai niihin liittyviin turvaamistoimenpiteisiin liittyvää. Kuitenkin tästä voidaan poiketa, jos rekisteröity itse on antanut suostumuksen tai sitä velvoittaa oikeudellinen syy. (Yleinen tietosuoja-asetus 2016, 9 artikla.)

Jos rekisterinpitäjä ei pysty tunnistamaan luonnollista henkilöä käsiteltävien tietojen pohjalta, ei rekisterinpitäjällä ole velvollisuutta hankkia lisätietoa, vain jos olisi tarpeen pystyä noudattamaan jotakin asetuksen säännöstä. (Yleinen tietosuoja-asetus 2016, 10 artikla.)

4.3 Rekisteröidyn oikeudet

Rekisterinpitäjällä on oltava läpinäkyvät sekä helposti saatavilla olevat toimintatavat rekisteröidyn tietoja tarvittaessa, kun rekisteröity niitä esimerkiksi oikeudellista syistä tarvitsee. Kaikki henkilötietoja koskeva tiedot ja viestit tulee toimittaa ymmärrettävässä muodossa sekä selkeällä ja yksinkertaisella kielellä, jossa otetaan huomioon rekisteröidyn tarpeet. (Yleinen tietosuoja-asetus 2016, 11 artikla.)

Kun rekisterin pitäjä kerää henkilötietoja, jotka koskevat rekisteröityä, on tällöin toimitettava rekisteröidylle vähintään seuraavat artiklan 14 mukaiset tiedot:

a) Rekisterinpitäjän, tämän edustajan sekä tietosuojavastaavan yhteystiedot,
b) henkilötietojen käsittelyn tarkoitukset, jotka sisältävät sopimusmääräykset ja sopimusehdot,
c) säilytysaika,
d) rekisteröidyn oikeus pyytää häntä koskevia tietoja rekisterin ylläpitäjältä sekä oikeus pyytää tietojen oikaisemista sekä poistamista,
e) oikeus valitukseen viranomaiselle sekä tämän yhteystiedot,
f) tietojen vastaanottajat,
g) tieto tietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, sekä tämän tarjoaman tahon tietosuoja taso,
h) kaikki muut tiedot, jotka takaavat asianmukaisen tietojen käsittelyn rekisteröidyn kannalta.

Rekisterinpitäjän tulee myös ilmoittaa edellisten kohtien lisäksi, onko tietojen kerääminen vapaaehtoista vai pakollista ja mitä tietojen antamatta jättämisestä seuraa. Jos henkilötietoja ei ole kerätty itse rekisteröidyltä, tulee rekisterinpitäjän ilmoittaa edellä mainittujen lisäksi mistä henkilötiedot on saatu. (Yleinen tietosuoja-asetus 2016, 14 artikla.)

Rekisteröidyllä tulee olla oikeus saada tietää, käsitelläänkö hänen tietojaan vai ei. Jos tietoja käsitellään, on hänellä oltava oikeus päästä käsiksi käsiteltäviin tietoihin, niiden tarkoitusperiin, käsittelyyn liittyviin tahoihin sekä säilytys menetelmiin. Rekisteröidyn itse pyydettäessä on rekisterinpitäjän toimitettava tiedot rekisteröidylle, rekisteröidyn pyytämällä tavalla. (Yleinen tietosuoja-asetus 2016, 15 artikla.)

4.4 Tietojen oikaiseminen ja poistaminen

Rekisteröidyn sitä vaatiessa, on rekisterinpitäjän ilman aiheetonta viivästystä oikaistava kaikki rekisteröityä koskevat epätarkat ja virheelliset tiedot. Tiedon käyttötarkoitukset huomioiden, on rekisteröidyllä oikeus saada puutteelliset tiedot täydennettyä esim. toimittamalla lisäselvitys. (Yleinen tietosuoja-asetus 2016, 16 artikla.)

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan häntä koskevat henkilötiedot järjestelmästä sekä rekisterinpitäjän on velvollisuus poistaa rekisteröityä koskevat tiedot ilman aiheetonta viivästystä, jos joku seuraavista täyttyy:

a) Henkilötietojen käsittelylle ei ole enää perusteita, jota varten ne kerättiin tai joita varten niitä käsiteltiin,
b) rekisteröity peruuttaa suostumuksena, eikä käsittelylle ole muuta laillista perustetta,
c) rekisteröity vastustaa käsittelyä, eikä käsittelyyn ole perusteltua syytä,
d) lainvastainen käsittely,
e) Unionin oikeuteen tai jäsenvaltioon lainsäädäntöön perustuvaan rekisterinpitäjää, koskevan lainsäädännön velvoitteen noudattamiseksi,
f) tiedot on kerätty tietoyhteiskunnan tarjoamien palvelujen yhteydessä, koskien alaikäisiä.

Rekisterinpitäjän julkistaessa tiedot on tällä velvollisuus rekisteröidyn pyytäessä tietojenpoistoa ilmoitettava muille osalliselle, joille tietoja on luovutettu. Kyseisiä henkilötietoja käsittelevien tahojen tulee poistaa henkilötietoihin liittyvät linkit, jäljennökset ja kopiot. Tähän tulee soveltaa käytettävissä olevaa teknologiaa sekä ottaa huomioon toteuttamiskustannukset. Edellä mainittuihin poistotarpeisiin ei ole tarvetta, jos käsittely on tarpeen koskien: sananvapautta, yleistä etua, lain velvoittamista, kansanterveyttä, oikeusvaadetta tai se vaikeuttaa oleellisesti yleisen edun mukaista arkistointitarkoituksen artiklan 89. määrittelemää käsittelyä. (Yleinen tietosuoja-asetus 2016, 17 artikla.)

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää rajoittamaan tietojenkäsittelyä, jos:

a) Rekisteröity kiistää tietojen paikkaansa pitävyyden, jolloin käsittelyä rajoitetaan niin kauan, että rekisterinpitäjä varmistaa tietojen paikkaansa pitävyyden,
b) käsittely on lainvastaista ja rekisteröity vastustaa tietojen poistamista ja pyytää niiden käsittelyn rajoittamista,
c) rekisterinpitäjä ei enää tarvitse tietoja, mutta rekisteröity tarvitsee niitä oikeudellisia toimia varten.

Tällöin tietoja saa käsitellä ainoastaan rekisteröidyn luvalla taikka tietoja tarvitaan oikeudellisen syyn vuoksi, toisen luonnollisen henkilön suojelemiseksi tai jäsenvaltion yleisen edun ylläpitämisen vaativan syyn vuoksi. Rekisterinpitäjän on myös ilmoitettava rekisteröidyn pyyntöä koskevan rajoittamisen poistamisesta rekisteröidylle. (Yleinen tietosuoja-asetus 2016, 18 artikla.)

Rekisterinpitäjän tulee ilmoittaa asianomaisille kaikista artiklan 16. ja 17. mukaisista muokkauksista henkilötietoihin. Tämä tarkoittaa myös niitä osapuolia joille tiedot ovat luovutettu, kuitenkaan sellaisessa tilanteessa tämä ei ole tarpeellista, jos se muodostuu mahdottomaksi tai vaatii kohtuuttomasti vaivaa. (Yleinen tietosuoja-asetus 2016, 19 artikla.)

Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä mm. suoramarkkinointia varten sekä myös vastustaa artiklan 89 mukaista käsittelyä, jolloin hänen tietojaan ei saa käsitellä, ellei huomattavan tärkeä ja perusteltu syy syrjäytä hänen etujaan. (Yleinen tietosuoja-asetus 2016, 21 artikla.)

Rekisteröidyllä on oikeus olla joutumatta automaattiseen tietojenkäsittelyyn, kuten profilointiin ja käsittelyihin, jotka vaikuttaisivat häneen koskeviin oikeusvaikutuksiin tai jotka *vaikuttavat häneen vastaavasti. (Yleinen tietosuoja-asetus 2016, 22 artikla.)*

5 MITÄ TARKOITTAA OIKEUS TULLA UNOHDETUKSI?

Tämän opinnäytetyön empiirinen selvitys käsittelee tietosuoja-asetuksen 679/2016 artiklaa 17., jonka mukaan rekisteröidyllä osapuolella on oikeus vaatia tietojensa poistoa rekisterinpitäjän ylläpitämästä henkilötietojärjestelmästä.

5.1 Tutkimuskysymys

Turun ammattikorkeakoulu esitti tietosuoja-asetuksesta tutkimusalueeksi *oikeus tulla unohdetuksi* maininnan. Aihetta lähdettiin lähestymään melko laajalta alueelta tietojen säilytyksen ja poiston kannalta. Lopuksi aihe kuitenkin rajattiin tarpeellisiin toimiin, kun rekisteröity ilmoittaa tahtonsa henkilötietojensa poistoon tietojärjestelmästä. Tutkimuksen kohteena oleva tietojärjestelmä oli organisaation tukipyyntöjärjestelmä.

5.2 Tutkimusmenetelmät

Opinnäytetyön aiheen ollessa kehittämistä olemassa olevaan järjestelmään, määrittyi sen tyyliksi konstruktiivinen tutkimusote. Tässä metodissa tarkoituksena on kehittää uutta todellisuutta, hyvin läheisessä tiimimäisessä yhteistyössä tutkijan ja käytännön edustajan välillä. (Kuikka, 2016.) Aihetta lähdettiin tutkimaan kartoittavasti, eli selvittiin mitä asioita tutkimukseen liittyy ja mistä saada tietoa, johon tutkimus pohjautuisi. Toimeksiantajan opastuksella käytettävää materiaalia löytyi runsaasti internetistä sekä kirjoista.

Tutkimuskysymyksen pohjautuessa tulevaan laki säädökseen oli lähtökohtana selvittää, mitä tämä asetus asettaa vaatimuksiksi henkilörekisterin pitäjälle. Tietosuoja-asetusta käytiin artikla kerrallaan läpi, ja sieltä poimittiin kaikki *oikeuteen tulla unohdetuksi* liittyvät tiedot. Tällä tavalla pystyttiin rakentamaan lista vaatimuksista ja kuvaus prosessista, joka kertoo, mitkä toimenpiteet tulee suorittaa, kun pyyntö saapuu.

5.3 Vaatimukset

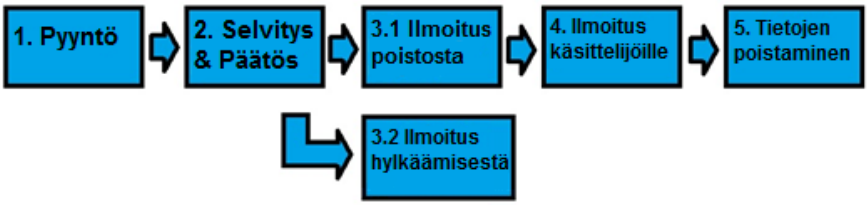
Euroopan Unionin tietosuoja-asetuksessa 679/2016 todetaan, että yksityisellä henkilöllä on oikeus tulla unohdetuksi tietojärjestelmästä. Tämä tarkoittaa sitä, että henkilö on rekisteröitynä tietokantaan ja tässä tietokannassa on henkilötietoja hänestä, jotka rekisteröity haluaa poistettavaksi kyseisestä tietokannasta. Henkilötiedoiksi luetaan kaikki tiedot, joista voidaan tunnistaa rekisteröity suorasti tai epäsuorasti. Rekisteröidyllä on vapaus käyttää tätä oikeutta artiklan 17. kohdan 1. perusteiden mukaisesti. Nämä perusteet sisältävät esimerkiksi tietojen käsittelyn tarpeettomuuden, rekisteröidyn suostumuksen peruuntumisen, laittomuuden tai alaikäisenä tapahtuneen tietojen keräämisen. (Yleinen tietosuoja-asetus 2016, 17 artikla.)

Tietoja käsittelevän osapuolen tulee ennen tietojen poistamisen prosessin aloittamista selvittää tietojen poistamisen tarpeellisuus. Asetuksessa on määriteltynä artiklan 17. kohdassa 3. poikkeus, joka mahdollistaa käsittelyn ja kumoaa kohdan 1. sovellutuksen. Vaatimuksena henkilötietojen käsittelyn jatkamiselle on, että se koskee sananvapauden ja tiedonvälittämisen vapautta, yleistä etua ajavaa tietojen käsittelyä, lakimääritteistä tietojenkäsittelyä tai oikeudellista toimea. (Yleinen tietosuoja-asetus 2016, 17 artikla.)

Tässä opinnäytetyössä oikeus tulla unohdetuksi määritettiin toimeksiantajan näkökulmasta käsittämään täydellistä henkilötietojen poistoa, eikä siihen sisällytetty poikkeuksia tietojen säilyttämiselle.

5.4 Prosessi

Oikeus tulla unohdetuksi vaatimuksen ymmärtämistä varten luotiin prosessikaavio, josta nähdään selvästi prosessin eri vaiheet rekisterinpitäjän näkökulmasta. Tämän kaavion avulla voidaan havainnoida, että prosessi on hyvin yksinkertainen ja mahdollisia lopputuloksia rekisteröidyn pyynnölle on kaksi. Ensimmäinen päätyy tietojen poistamiseen järjestelmästä ja toisessa rekisterinpitäjä on pitänyt oikeutensa jatkaa tietojen käsittelyä asetukseen nojaten. Tämä koko prosessi rekisteröidyn pyynnöstä on asetuksen mukaan toteutettava ilman aiheetonta viivästystä, on päätös tietojenpoistamisesta kumpi tahansa.



Kuvio 1. Oikeus tulla unohdetuksi-pyynnön prosessi

Kuvion 1. kohdassa 1. todetaan, että rekisteröity käyttää oikeuttaan tulla unohdetuksi tietojärjestelmästä ja tekee tietoja käsittelevälle rekisterinpitäjälle pyynnön tietojen poistamisesta. Tämän pyynnön toimittamisen jälkeen siirrytään kohtaan 2., jolloin rekisterinpitäjä vastaanottaa pyynnön. Tämä tarkoittaa rekisterinpitäjän kannalta selvitystä omasta tietojen käsittelyn tarpeellisuudesta, ja onko asiakkaana olevan rekisteröidyn pyyntö aiheellinen.

Rekisterinpitäjä on tehnyt päätöksen asiasta, ja siirrytään kuviossa seuraavaan kohtaan. Tietojen poistamisen tapauksessa edetään kohtaa 3.1., joka käsittää rekisterinpitäjän ilmoitusvelvollisuuden tietojen poistamisesta. Tämä tarkoittaa ilmoitusta rekisteröidylle, tietojen poistamisen toteutumisesta. Kohdassa 3.2. olevan päätöksen ollessa kielteinen tietojen poistamisen osalta on rekisterinpitäjän ilmoitettava tästä rekisteröidylle. Tähän on hyvä antaa selvitys kyseiseen lopputulokseen johtaneista syistä.

Myönteisen poistamisen seurauksena oleva kohta 4. sisältää ilmoituksen kolmansille osapuolille, joille se on mahdollisesti luovuttanut tietoja eteenpäin. Tietoja käsittelevät kolmannet osapuolet joutuvat poistamaan omat rekisteröityä koskevat henkilötiedot. Näihin toimiin tulee kuitenkin ottaa huomioon käytettävissä olevat kohtuulliset toimenpiteet.

Viimeisessä kohdassa (5.) on tekniset toimenpiteet, jotka rekisterinpitäjän tulee suorittaa tietojen poistamiseksi. Ylläpitäjällä tulee olla selkeä tietämys, missä kaikkialla kyseisiä henkilötietoja on järjestelmässä säilytetty, ja kuinka ne pystytään sieltä poistamaan.

6 TIETOJEN POISTAMINEN JÄRJESTELMÄSTÄ

Tämän osion tarkoituksena on syventyä tietojen poistamiseen tekniseltä kannalta, ja selvittää kuinka tietojen poistaminen on käytännössä mahdollista tietokannasta. Tämä selvitys on tehty yhden tietyn tietojärjestelmän näkökulmasta, ja sen käyttäminen toiseen järjestelmään ei välttämättä ole sellaisenaan mahdollista. Kuitenkin samoja periaatteita voidaan soveltaa vastaaviin järjestelmiin.

Opinnäytetyön tilanneella Turun ammattikorkeakoululla oli käytössä avoimeen lähdekoodiin perustuva OTRS -tiketinhallintajärjestelmä. Tämä järjestelmä sisältää SQL -tietokannan, ja sitä käytetään selainpohjaisella käyttöliittymällä. Sovelluksen periaate on tarkastella ja hallita asiakkaiden lähettämiä tikettipyyntöjä. Tiketti on eräänlainen työpyyntö, joka sitten lähetetään asiaankuuluvalle taholle. Tämä taho näkee tiketit järjestelmässä luettelomaisesti, jolloin niitä pystytään seuraamaan kätevästi. Lisäksi niihin pystytään vastaamaan, jolloin viesti menee suoraan asiakkaalle. Näitä tikettejä pystytään siirtämään eteenpäin eri työjonoihin ja eri käyttäjille, jos työpyyntö vaatii useampia tekijöitä.

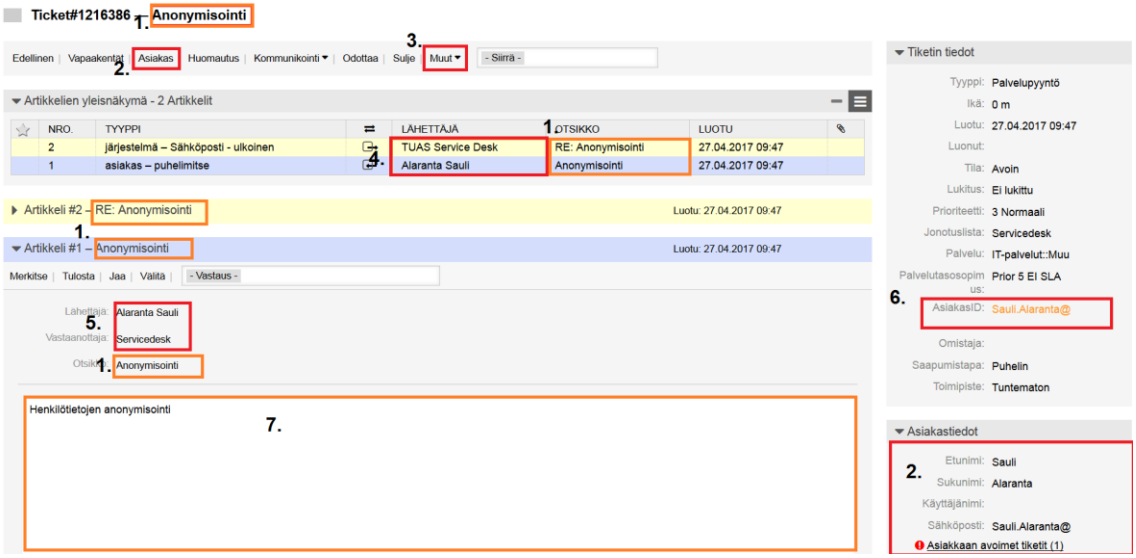
Tarkoituksena oli selvittää tietojen poistaminen asetuksen näkökulmasta, sekä kuinka tietojen poistaminen pystytään toteuttamaan käytännössä järjestelmässä, jotta toimeksiantajan määrittelemä oikeus tulla unohdetuksi voidaan pyynnöstä suorittaa.

Toimeksiantajan puolelta työni apuna oli kaksi järjestelmän ylläpitäjää, joiden kanssa muodostimme projektiryhmän, ja heidän avulla oli mahdollista syventyä enemmän tikettijärjestelmän toimintaan. Ylläpitäjien apu oli tärkeää, sillä järjestelmän admin eli ylläpitäjänäkymään on vain muutamilla henkilöillä oikeus, sekä heillä oli tarvittava asiantuntemus järjestelmän toiminnasta.

6.1 Vaatimukset

Toimeksiantajalla oli toiveita tietojen poistamisen kannalta. Tärkeimpänä oli mahdollisuus säilyttää mahdollisimman paljon tietoa asiakkaan tiketeistä tilastointitarkoitusta silmällä pitäen. Tikettien tiedolla tarkoitetaan tässä opinnäytetyössä niiden aikaleimoja, muutoshistoriaa ja tikettien viestiketjujen rakennetta. Tämän lisäksi tietojen poistoa tuli tarkastella tietosuojan toteutumisen näkökulmasta, ja sen tarjoamista mahdollisuuksista.

Tikettijärjestelmässä olevaa tietoa tutkittiin selainkäyttöliittymän avulla. Yhdessä projektiryhmän kanssa totesimme, että henkilötietojen sijainnit pitää ensiksi kartoittaa, jotta pystytään kehittämään jatkotoimenpiteitä tietojen poistolle. Nämä henkilötietoja sisältävät kohdat pystytään näkemään kuvassa 1., jossa on ympyröity punaisella henkilötietoja *sisältävät* tietueet, ja oranssilla on ympyröity tietueet, joissa *saattaa* olla henkilötietoja.



Kuva 1.OTRS -tiketin henkilötietojen sijainnit (OTRS 5)

Kuvassa 1. on esitetty yksittäisen tiketin rakenne. Henkilötietoja sisältävät kohdat selitettynä:

1. Tiketin otsikko, joka sisältää mahdollisesti henkilötietoja. Riippuen, miten asiakas on sen nimennyt.
2. Asiakastiedot, joka sisältää kaikki yhteystiedot asiakkaasta.
3. Historia listaus, joka sisältää kaikki muutokset tikettiin.
4. Yleisnäkymä, joka sisältää lähettäjän nimen ja tiketin otsikon.
5. Yhteystiedot, joka sisältää lähettäjän, vastaanottajan sekä tiketin otsikon.
6. Tiketin tiedot, joka sisältää asiakas ID numeron ja mahdollisesti muuta henkilötietoa.
7. Tiketin sisältö, joka sisältää mahdollisesti henkilötietoa, liitteitä ja viesti kopioita.

Tiketin viestihistoria muodostuu artikkeleista, jotka sisältävät esimerkiksi viestikenttiä (kenttä 7.). Toimeksiantajan haluna on säilyttää viestikenttien järjestys, aikaleimat ja muut tiedot, mutta poistaa niistä henkilötiedot. Nämä edellä mainitut artikkelit pystytään

löytämään myös OTRS database schema eli OTRS -tietokantarakenne nimisestä julkisesta taulukosta. (OTRS 5 2015). Kyseinen taulukko on tietokanta kaavio, jossa on kuvattu koko järjestelmän tietokannan osat ja niiden linkittymät. Taulukon tulkitseminen on hankalaa sen monimutkaisuudesta johtuen, joten sitä tutkittiin yhdessä ylläpitäjän kanssa.

6.2 Hypoteesit

Ensimmäiseksi pohdittiin vaihtoehtoja tietojen säilyttämisen ja poistamisen kannalta. Seuraavassa on listattuna tietojen säilyttämisen hypoteeseja, jotka pohjautuvat tietosuoja-asetukseen 679/2016, käyttökokemuksiin sekä tuntemuksiin järjestelmästä, ja ne on luotu yhdessä projektiryhmän kanssa.

Tapa 1: *Asiakastietojen poisto tarpeellisen ajan jälkeen tiketistä*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, siitä poistetaan asiakastiedot (Kuva 1.). Tämä tapahtuu muuttamalla asiakkaan tietojen tilalle ennalta määritetty anonyymi-käyttäjä. Positiivista tässä menetelmässä on tiketin rakenteen, ja tilastointitietojen säilyminen, mutta jäljelle jää mahdollisesti myös henkilötietoja viestikenttiin ja historia-lokiin. Tässä menetelmässä ei toteutuisi toimeksiantajan määrittelemä oikeus tulla unohdetuksi, mahdollisesti jäljelle jäävien tietojen vuoksi.

Tapa 2: *Tietojen pseudonymisointi*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, siitä muutetaan tunnistettavat henkilötiedot pseudonymisoiduiksi. Tämä tapahtuu muokkaamalla asiakkaan tunnistettavat henkilötiedot yksistään tunnistamattomaksi arvoksi ohjelman tietokannassa, jolloin asiakasta ei pystytä tunnistamaan tiedoista ilman lisätunnisteita. Kaikki tunnistetiedot siirretään erilliseen ja tarkemmin suojattuun tietokantaan, josta asiattomat käyttäjät eivät pysty saamaan niitä käsiin. Tässä menetelmässä on positiivista mahdollisuus tietojen yhdistämiseen ja hyödyntämiseen tulevaisuudessa, sekä tietosuoja-asetus 679/2016:n oletuskohtainen sisällytetty tietosuoja pseudonymisoinnista toteutuu. (Yleinen tietosuoja-asetus 2016, 25 artikla).

Negatiivista on kuitenkin pseudonymisoinnin sopimattomuus tiedon säilyttämisen loppuratkaisuna, sillä tietosuoja-asetuksen mukaan myös pseudonyymi tieto on henkilötietoa, ja sitä ei saa säilyttää käsittelyn tarpeellisuuden jälkeen (Tarhonen 2017). Oikeus tulla unohdetuksi ei toteutuisi tässä menetelmässä, sillä toimeksiantajan tavoitteena on henkilötietojen täydellinen poisto.

Tapa 3: *Arkistointi*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, se siirretään arkistoon. Tämä arkisto olisi erillinen tietokantapalvelin, jossa toteutuu korkeampi tietoturvataso, ja vain tietyillä käyttäjillä olisi oikeudet siihen. Tietosuoja-asetuksen 679/2016 artiklan 89. mukaan on mahdollista siirtää henkilötiedot arkistoon, jos se ajaa yleistä etua, ja jos sitä käytetään tieteellisiin, tilastollisiin tai historiallisiin tarkoituksiin. Nämä tiedot tulisi kuitenkin minimoida, sekä niiden säilyttämistä tulee harkita säännöllisin väliajoin. (Yleinen tietosuoja-asetus 2016, 89 artikla). Rekisterinpitäjän kannalta tässä tavassa olisi erittäin hyvä tietojen hyödyntämisen mahdollisuus tilastoinnin kannalta, mutta on harkinnanvaraista, täyttyykö arkistoinnin määritelmät oman tietojensäilytyksen tarpeen kannalta. Tässä menetelmässä ei toteutuisi toimeksiantajan määrittelemä oikeus tulla unohdetuksi, johtuen mahdollisesti jäljelle jäävien tietojen säilymisestä, sillä niitä ei poisteta ollenkaan lähtökohtaisesti.

Tapa 4: *Tiketin poisto ja luonti uudelleen tilastointia varten*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, niin siitä tehdään kopio tikettijärjestelmään, mutta henkilötiedot poistetaan kokonaisuudessaan. Alkuperäinen tiketti poistetaan järjestelmästä. Menetelmässä on positiivista tietojen poistuminen kokonaisuudessaan. Toimeksiantajan määrittelemä oikeus tulla unohdetuksi toteutuu tässä menetelmässä. Pitää huomioida, että vain osa tilastointitiedoista jää jäljelle. Aikaleimat ja viestirakenne menetetään.

Tapa 5: Tunnistettavien tietojen muokkaus anonymisoiduksi

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, niin sitä muokataan henkilötietojen osalta täysin anonymisoiduksi. Tämä on hyvin samantapainen menetelmä kuin pseudonymisoinnissa, mutta tietoja ei pystytä enää yhdistämään, vaan ne on muokattu tunnistamattomaksi eli

anonyymiksi lopullisesti. Tässä menetelmässä on positiivista tiketin rakenteen ja tilastointitietojen säilyminen. Toimeksiantajan määrittelemä oikeus tulla unohdetuksi pystytään myös toteuttamaan tällä tavalla.

Tapa 6: *Tiketin käsittelyn rajoittaminen*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, sen käsittelyä rajoitetaan. OTRS -järjestelmässä on mahdollista toteuttaa tämä kahdella eri tapaa. Se joko siirrettäisiin toiseen jonoon, jossa sen käyttöoikeuksia rajoitettaan, tai se siirretään OTRS -arkistointitoimintoon, joka poistaa sen näkyvistä käyttäjiltä. Tämä olisi helppo toteuttaa, koska järjestelmä sisältää jo nämä ominaisuudet. Toimeksiantajan määrittelemä oikeus tulla unohdetuksi ei kuitenkaan toteudu tällä menetelmällä, sillä henkilötietoja ei poisteta järjestelmästä.

Tapa 7: *Tilastotietojen kerääminen ja henkilötietojen poisto automaattisesti*

Tiketti saapuu järjestelmään asiakkaan toimesta, ja se käsitellään normaalisti. Kun tiketin käsittely ei ole enää tarpeellista, siitä kerätään ylös tilastointi tiedot OTRS -järjestelmän raportointityökalulla. Tämän jälkeen tiketti poistetaan järjestelmästä. Tätä pystytään hyödyntämään myös suurille määrille tikettejä, jolloin säännöllisin väliajoin kerätään tietoja tiketeistä, ja ne poistetaan kuormittamasta järjestelmää. Positiivista on tilastointitietojen järjestelmällinen kerääminen, ja tikettien poisto lähtökohtaisesti koko järjestelmästä. Toimeksiantajan määrittelemä oikeus tulla unohdetuksi toteutuu tässä tavassa.

6.3 Vaihtoehtojen rajaus

Vaihtoehtoja verrattiin keskenään projektiryhmän kesken, ja niistä valikoitiin kolme parhaiten sopivaa jatkoselvitystä varten. Nämä kolme vaihtoehtoa olivat: 5. tunnistetavien tietojen muokkaaminen anonyymisoiduksi, 6. tiketin käsittelyn rajoittaminen sekä 7. tilastotietojen keräys ja tietojen poisto automaattisesti. Tämä jatkoselvitys toteutettiin taulukkona, jossa oli listattuna toimeksiantajan antamia vaatimuksia, säilytyksen toteutumiselle. Vastaus vaihtoehdot olivat kyllä ja ei, riippuen toteutuuko vaatimus kyseisessä tavassa.

Vertailussa vaihtoehto 7. eli tiketin käsittelyn rajoittaminen karsittiin jo alkuvaiheessa pois, johtuen sen huonosta soveltuvuudesta, kun sitä vertailtiin 5. ja 7. vaihtoehtoihin.

Jäljelle jäävät vaihtoehdot olivat molemmat toimeksiantajan mielestä hyviä, sillä molemmista löytyi omat vahvuutensa toteutuksen kannalta.

	5.Tunnistettavien tietojen muokkaus anonymisoiduksi	6. Tiketin käsittelyn rajoittaminen	7. Tilastotietojen keräys ja tietojen poisto automaattisesti
Tiketti säilyy järjestelmässä	Kyllä	Kyllä	Ei
Lähes kaikki tarpeellinen tieto tiketistä käytettävissä (rakenne yms.)	Kyllä	Kyllä	Ei
Tilastotietoja käytettävissä (aika, jonot)	Kyllä	Kyllä	Kyllä
Tietojen palautus mahdollinen	Ei	Kyllä	Ei
Oikeus tulla unohdetuksi sisältyy	Kyllä	Ei	Kyllä
Haluttujen tikettien valinta mahdollista	Kyllä	Kyllä	Kyllä

Taulukko 1. Jatkoselvityksen vertailu

Viidennessä vaihtoehdossa eli anonymisoinnissa, vahvuutena oli tikettien tietojen hyödynnettävyys tulevaisuudessa, tiketin viestien rakenteen ja tilastotietojen osalta. Kuitenkin tämä vaihto vaatisi erikseen selvitystyötä tietojen paikallistamisen ja muokkauksen osalta. Seitsemännessä vaihtoehdossa oli vahvuutena sen helppous, sillä raportointi tie-

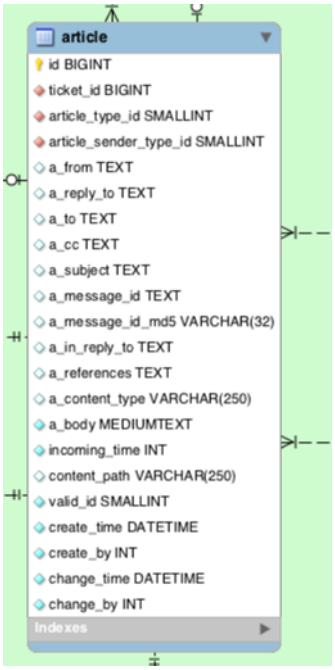
don kerääminen ja tiketin poiston vaatimattomuus eivät vaatisi paljoa työtä. Lisäksi menetelmän laillisuutta asetuksen kannalta ei tarvitsisi miettiä, sillä henkilötietoja ei järjestelmään jää.

Lähempään tarkasteluun valittiin vaihtoehto 5., sillä tämän tavan kokeileminen järjestelmään olisi tietojen hyödyntämisen kannalta parempi vaihtoehto. Vaikka ratkaisutapa vaatisi enemmän työtä, niin sen toimimisen tulosten selvittäminen järjestelmässä olisi tulevaisuutta ajatellen kannattavampi. Seitsemännen vaihtoehdon kohdalla ei selvittämistä olisi paljoa, sillä toimeksiantajalla on jo tieto ja osaaminen, kuinka se toteutetaan.

6.4 Anonymisointi

Toimeksiantajan päätöksen mukaan valitusta kehitysideasta tehtiin PoC eli proof of concept -versio. Tämä tarkoittaa idean suunnittelua demomaisesti, ja tarkoitus oli kokeilla, miten anonymisoinnin idea toimii käytännössä. PoC -vaiheen jälkeen päätetään tulosten perusteella, onko idea toteutuskelpoinen vai kaipaako se lisää hiomista. (Omnipartners, 2017.)

Tämä vaihe toteutettiin projektiryhmän asiantuntijoiden avulla, ja he selvittivät, kuinka tietoja pystytään käytännössä muuttamaan. Tämä anonymisoinnin suunnitelma perustui kuvan 1. (s.27) tikettinäkymään, joka sisältää OTRS -järjestelmän tietojen sijainnit käyttöliittymässä. Punaisin ja oranssein rajatuissa kohdissa olevat tiedot haettiin taustalla pyörivältä tietokantapalvelimelta. Käytännössä tarvittavia muutososa-alueen kohteita oli 3, asiakastiedot, tikettitiedot ja historia.



Kuva 2. OTRS 5 -tietokantarakenteen article-taulu (OTRS 5)

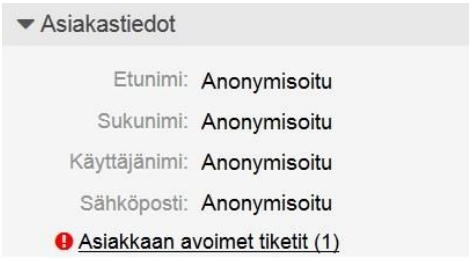
Nämä tietokannan osien nimet pystytään paikallistamaan OTRS -tietokantakaaviosta (kuva 2). Käyttöliittymän SQL -kyselytoiminto ominaisuuden avulla pystyttiin tarkastelemaan haluttujen solujen arvoja. Esimerkiksi tikettitiedot löytyivät tietokannasta *article* taulusta, ja historia *ticket_history* taulusta.

6.4.1 Asiakastiedot

Helpoin selvityskohta oli asiakastietokentät, josta löytyvät kaikki asiakkaaseen liittyvät tiedot. Tämä muokattiin vaihtamalla asiakkaaksi toinen anonyymi käyttäjä, jolloin asiakastietokentistä poistui alkuperäiset henkilötiedot. Tämä menetelmä asiakastietojen anonymisointiin ei tarvinnut SQL -tietokannan muutoksia.

Kuva 3.Asiakaskäyttäjä vaihdettuna anonyymi käyttäjään (OTRS 5)

Kuvassa 3. oleva valikko löytyi tiketin Asiakas-valikosta, ja asiakaskäyttäjää muuttamalla voidaan asiakkaan tiedot vaihtaa toiseen. Tässä tapauksessa ne on vaihdettu anonymisoitu-käyttäjäksi.



Kuva 4. Asiakastiedot ovat muuttuneet tiketissä (OTRS 5)

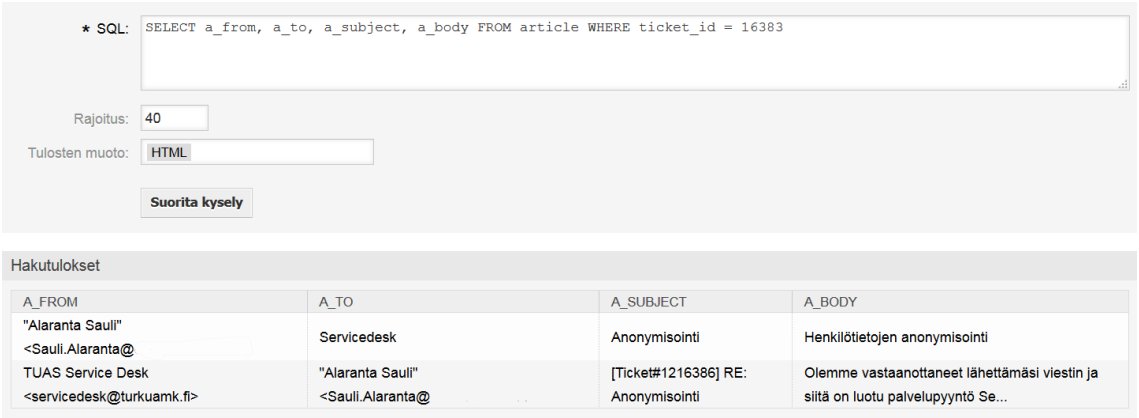
Kuvassa 4. olevat muutokset vaikuttivat myös tiketissä olevaan asiakastiedot-kenttään, ja muuttivat sen käyttäjän tiedot toiseksi. Näin tiketin asiakastiedoista ei pystytä enää tunnistamaan alkuperäistä asiakasta. Kuvaan 4. on hahmoteltu, miltä anonymisoitu käyttäjä näyttäisi asiakastietokentässä.

6.4.2 Tikettitiedot

OTRS ohjelmassa käytettäviä tietoja pystyttiin lukemaan käyttöliittymässä olevalla SQL -tietotokannan kyselytoiminnolla. Se toimii normaaleilla SQL -komennoilla, mutta ainoastaan lukutilassa, eli arvoja ei tätä kautta pystytty muuttamaan. Artikkelien arvot, jotka haluttiin tässä tapauksessa muuttaa, olivat A_FROM, A_TO, A_SUBJECT ja A_BODY. Nämä kohdat joko sisälsivät henkilötietoja tai olivat kohtia, joista mahdollisesti löytyy kyseisiä tietoja. Tiedot saatiin esiin syöttämällä komento:

SELECT a_from, a_to, a_subject, a_body FROM article WHERE ticket_id = 16383

SELECT-komennolla kohdennetaan kysely haluttuihin artikkeleihin, jotka on listattu sen perään. *FROM*-komennolla kohdennetaan haku artikkeleihin. *WHERE*-komennolla määritellään tietty tiketti ID, johon tarkastelu halutaan kohdentaa.



Kuva 5. SQL -tietokanta kysely työkalu (OTRS 5)

Haetut kohteet listautuvat näkymään (kuva 5), jos niille löytyy vastine SQL -tietokannasta. Tässä tapauksessa kuvan 5. hakutuloksissa pystytään huomaamaan henkilötietoja, jotka löytyvät samanlaisina tiketistä.

Kun tietoja on tarpeellista muokata, se tulee tehdä suoraan tietokantaan. Tässä tapauksessa tarpeellista oli muokata kaikki kuvan 5. haun tulokset eli A_FROM, A_TO, A_SUBJECT ja A_BODY. Tämä tapahtui ottamalla yhteys tietokantapalvelimeen, ja sieltä syötettiin komennot, jotka muuttivat kyseiset arvot halutuiksi. Arvot voidaan muokata käyttämällä scramble-menetelmää, eli sekoittaa kokonaan, tai muokata halutuksi anonyymi -tunnisteeksi. Tietojen muokkaamiseen käytettiin seuraavia komentoja:

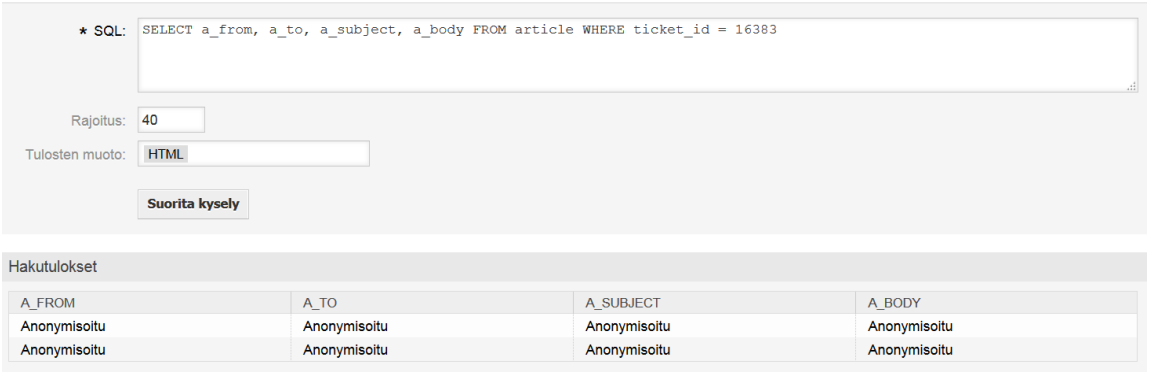
UPDATE article SET A_FROM='Anonymisoitu' WHERE TICKET_ID=16383;

UPDATE article SET A_TO='Anonymisoitu' WHERE TICKET_ID=16383;

UPDATE article SET A_SUBJECT='Anonymisoitu' WHERE TICKET_ID=16383;

UPDATE article SET A_BODY='Anonymisoitu' WHERE TICKET_ID=16383;

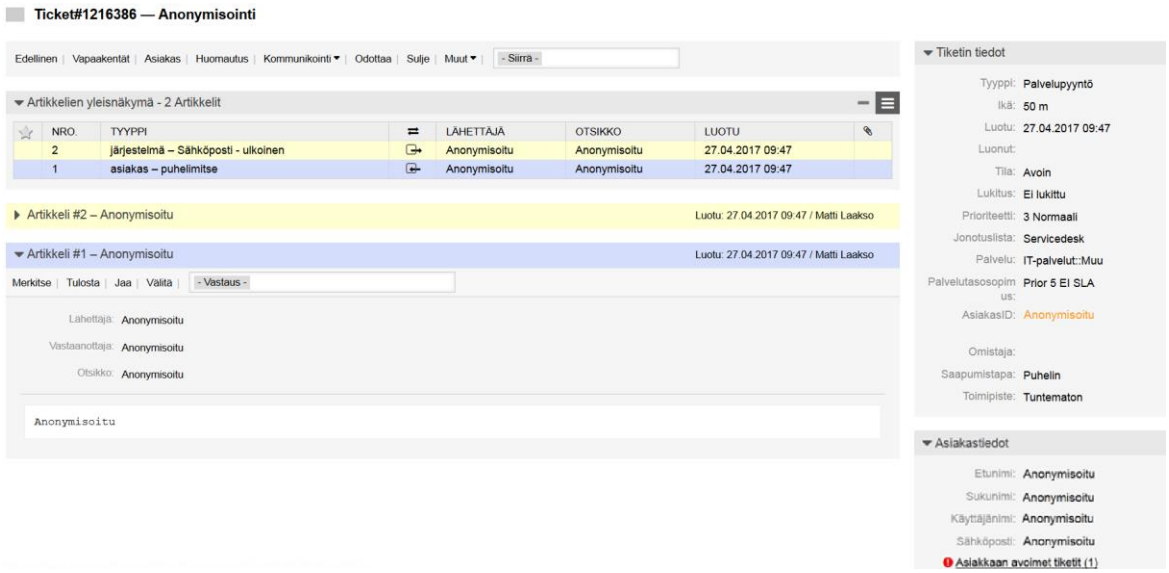
UPDATE-komennolla määrättiin kohdennus artikkeleihin, ja *SET*-komennolla asetettiin tietty artikkelin arvot muuttumaan anonymisoiduksi. *WHERE*-komento ohjasi muutoksen vain tiettyyn tikettiin.



Kuva 6. SQL -tietokannassa arvot ovat muuttuneet anonyymiksi (OTRS 5)

Tietokantapalvelimelle ajettujen arvojen muutosten jälkeen tietoja haettiin uudelleen, ja tällä kertaa ne ilmestyivät hakutulokset-näkymään anonyymeiksi muuttuneina (kuva 6).

Muuttuneet arvot pystytään nyt näkemään myös tiketti näkymässä (kuva 7), jossa tiket-titiedot ja asiakastiedot ovat muuttuneet anonyymiksi.



Kuva 7. Tiketin tiedot ovat muuttuneet (OTRS 5)

6.4.3 Historia

Tiketin vaiheita pystytään seuramaan sen historialistauksesta, johon tallentuu lokimaisesti kaikki siihen tehdyt arvojen muutokset, kuten kuvassa 8. voidaan havaita. Lista saatiin näkymään muut-pudotusvalikon historia-napista.

Kuva 8. Tiketin historia (OTRS 5)

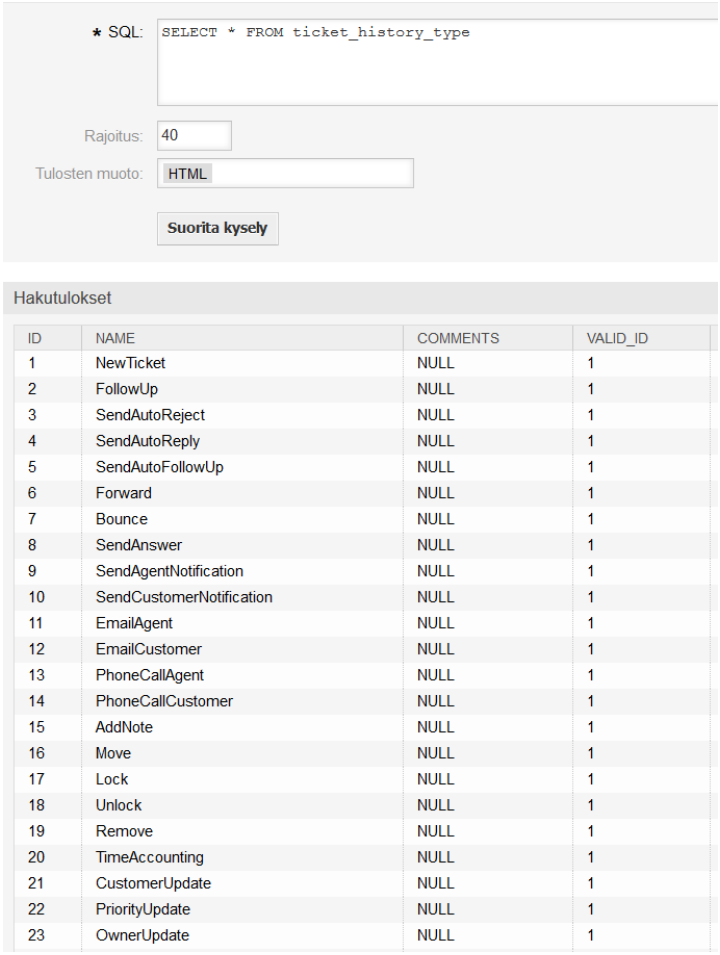
Listassa on monia mahdollisia käytettäviä tapahtumakohtia, jotka ilmestyvät listaan sen mukaan, kun niiden määrittelemiä arvoja käsitellään tiketissä. Kuvasta on ympyröity CustomerUpdate -tietue, joka sisältää asiakkaan sähköpostiosoitteen. Historian muokkaamista kokeiltiin tälle arvolle, ja sen käyttöä voidaan soveltaa muihin kohtiin listassa, jos on tarpeellista.

Listaus näistä tapahtumista löydetään OTRS -tietokantakaaviosta, jossa niiden taulun otsikkona toimii TICKET_HISTORY_TYPE. Tämä listaus saatiin näkymään kyselytoiminnolla, asettamalla komennoksi:

SELECT * FROM ticket_history_type

Tapahtumalistauksesta (kuva 9) pystytään näkemään kyseinen CustomerUpdate-tunniste eli ID 21. Tätä arvoa pystytään muuttamaan tietokantapalvelimella samaan tapaan, kuin tiketin tietoja, mutta pienellä *AND*-lisäyksellä, joka kohdentaa muutoksen vain kohtaan 21, CustomerUpdate. Kokonaisuudessaan komento on:

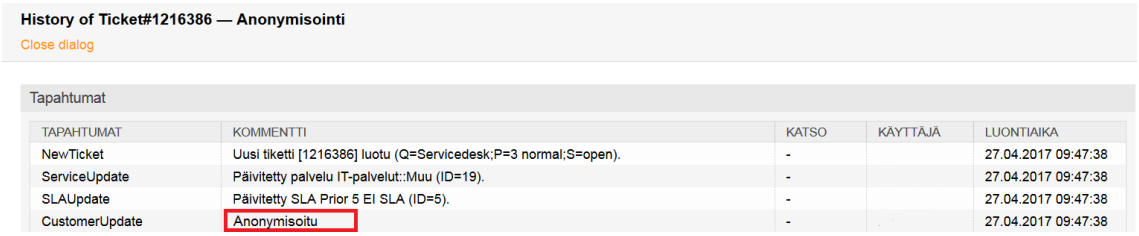
UPDATE ticket_history SET name='Anonymisoitu' WHERE ticket_id=16383 AND history_type_id=21;



ID	NAME	COMMENTS	VALID_ID
1	NewTicket	NULL	1
2	FollowUp	NULL	1
3	SendAutoReject	NULL	1
4	SendAutoReply	NULL	1
5	SendAutoFollowUp	NULL	1
6	Forward	NULL	1
7	Bounce	NULL	1
8	SendAnswer	NULL	1
9	SendAgentNotification	NULL	1
10	SendCustomerNotification	NULL	1
11	EmailAgent	NULL	1
12	EmailCustomer	NULL	1
13	PhoneCallAgent	NULL	1
14	PhoneCallCustomer	NULL	1
15	AddNote	NULL	1
16	Move	NULL	1
17	Lock	NULL	1
18	Unlock	NULL	1
19	Remove	NULL	1
20	TimeAccounting	NULL	1
21	CustomerUpdate	NULL	1
22	PriorityUpdate	NULL	1
23	OwnerUpdate	NULL	1

Kuva 9. Historia -lista, ja sen käytössä olevien tapahtumien arvot (OTRS 5)

Haluttujen arvojen ajamisen jälkeen SQL -tietokantaan, on mahdollista nähdä muuttuneet tiedot historia-listassa, kuten kuvassa 10.



TAPAHTUMAT	KOMMENTTI	KATSO	KÄYTTÄJÄ	LUONTIAIKA
NewTicket	Uusi tiketti [1216386] luotu (Q=Servicedesk;P=3 normal;S=open).	-		27.04.2017 09:47:38
ServiceUpdate	Päivitetty palvelu IT-palvelut::Muu (ID=19).	-		27.04.2017 09:47:38
SLAUpdate	Päivitetty SLA Prior 5 EI SLA (ID=5).	-		27.04.2017 09:47:38
CustomerUpdate	Anonymisoitu	-		27.04.2017 09:47:38

Kuva 10. Anonymisoitu CustomerUpdate tieto (OTRS 5)

Tätä menetelmää pystytään käyttämään myös muihin historia-arvoihin, kun tiedossa on halutun historiatyypin ID -numero.

6.5 Yhteenveto

Henkilötietojen anonymisointi käyttöliittymätasolla onnistui suunnitellusti, suunniteltuja menetelmiä käyttäen. Tällä tavoin tiedot ovat normaali OTRS -käyttäjälle anonymisoituja, ja henkilöä ei niistä pystytä tunnistamaan. Selvityksen aikana kuitenkin selvisi, että anonymisointi ei muokannut kaikkia tietoja, sillä tiedostojärjestelmään jää talteen henkilötietoja tiedosto- ja kansiorakenteeseen. Tämä johtuu ohjelman kehittäjän ratkaisuista, sillä osa tiedoista jää vielä palvelimelle talteen. Tämä johtaisi käytännössä siihen, että tiedot olisi vielä mahdollista yhdistää jäljelle jääviä tunnisteita käyttäen, eli ne olisivat tavallaan pseudonymisoituja.

Ratkaisuna tähän voisi olla anonymisoinnin jatkokehittäminen, esimerkiksi erillisen OTRS -lisäosan muodossa, joka poistaisi jäljelle jäävät tiedot myös kansiorakenteista. Tämä vaatii lisäselvittämistä tietojen sijainnin osalta, sekä ohjelmointia sovelluksen kehittämiseksi. Tämä olisi kenties kannattava kehityssuunnitelma tietyissä tilanteissa, jos osaamista ja työvoimaa tällaiseen löytyy. Pitää kuitenkin ottaa huomioon anonymisoinnin tarjoamien hyötyjen kannattavuus, jos tietojen säilyttämiselle ei olisikaan todellisuudessa riittävää syytä. Vaihtoehto ratkaisuiksi voisikin harkita vaihtoehtoja 7., eli tilastotietojen kerääminen ja tiketin poisto, tai vaihtoehtoa 4., eli tiketin kopiointi. Nämä vaihtoehdot olisivat hyödyllisiä tilastointitietojen osalta, sekä ne olisivat helpompia toteuttaa järjestelmässä. Tiketin kopiointia voisi selvittää myös vanhojen aikaleimojen osalta, sillä jopa se olisi helpompi toteuttaa, kuin totaalinen tietojen anonymisointi. Kopiointi-vaihtoehdon voisi nimetä esimerkiksi tiketin kloonaukseksi. Tiketti kloonattaisiin vanhojen tilasto- ja rakennetietojen perusteella niin, että se ei sisältäisi enää henkilötietoja.

7 PÄÄTELMÄT

Tutkimuksen tarkoituksena, oli selvittää mitä EU:n tietosuoja-asetuksessa 697/2016 oleva oikeus tulla unohdetuksi tarkoittaa, sekä kuinka se voitaisiin toteuttaa toimeksiantajan järjestelmässä. Työ tuli tilauksena Turun ammattikorkeakoululta, kun olimme pohtineet sopivaa opinnäytetyöaihetta ollessani siellä harjoittelussa. Harjoitteluni tapahtui juuri kyseisessä ammattikorkeakoulun Service Desk -tiimissä, ja käytännön kokemusta OTRS -järjestelmästä oli kertynyt tämän seurauksena jo jonkin verran.

Tutkimuskysymystä lähdin selvittämään enemmänkin tietosuoja-asetuksen näkökulmasta, sillä tästä aiheesta ei aikaisempaa kokemusta henkilökohtaisesti ollut. Lähdeaineistoa ei julkaistusta kirjallisuudesta paljoa löytynyt, ainakaan suomalaisilta tekijöiltä. Muutama alan käsikirja mainitsi asetuksen saapumisesta muutamalla sivulla, mutta syvällisempää katselmusta ei tutkimuksen aikana omiin käsiini löytynyt. Tämän vuoksi materiaali oikeuteen tulla unohdetuksi painottui pääsääntöisesti itse asetukseen, ja sen tulkitsemiseen. Asetuksen ymmärtäminen tuntui sen laajuutensa vuoksi alkuun hyvin raskaalta, mutta oikeat artikkelit sieltä löydettyä, se muuttui hyvin helppolukuiseksi, loogiseksi ja vaivattomaksi käsitellä omassa työssä.

Lähestyin oikeutta tulla unohdetuksi mainintaa myös internetin välityksellä, ja sieltä löytyikin helposti muutamia termien selityksiä asetuksen kannalta, kuten pseudonymisointi. Pystyin käyttämään hankittuja tietoja hyväksi tehdessäni omaa ”tulkintaa” oikeudesta tulla unohdetuksi. Kuitenkin asetuksen ollessa vasta ohjeistus EU:n jäsenvaltioille, on jokainen tulkinta vasta askel kohti mahdollista laillista ratkaisua. Siirtymävaiheen päättyessä toukokuussa 2018 on kenties mahdollista, että myös Suomeen saadaan lähiaikoina valtion virallinen näkemys asetuksesta, joka sitten lakiin vahvistetaan.

Aiheen laajuus tuotti haasteita tutkimustyön rajauksessa. Tutkimuskysymystä tehdessä, idea pyöri lähtökohtaisesti järjestelmän muokkaamisessa yrityksen käytössä olevan live järjestelmän osalta, eikä vain testipuolella. Tämä olisi tarkoittanut testattua ja toimivaa ratkaisua, jotta sen olisi voinut julkaista. Tähän olisi liittynyt myös tietojen säilyttäminen kokonaisuudessaan, joka on hyvin laaja aihealue toteutettavaksi, eikä opinnäytetyössä ollenkaan kannattava. Lisäksi omakohtainen osaaminen SQL -tietokantojen kanssa rajoittui AMK:n kursseilla opetettuihin perusteisiin. Lopuksi aihe saatiin rajattua sopivaksi, kun visio lopputoteutuksesta saatiin selkeäksi.

Lopputulokseen olen omalta osaltani hyvin tyytyväinen, sillä toimeksiantajan toiveet tulivat toteutetuksi opinnäytetyön vaatimusten osalta. He pystyvät hyödyntämään opinnäytetyön aikana selvitettyjä tutkimustuloksia oman toimintansa kehittämiseksi. Vaikka laatimamme hypoteesit eivät välttämättä olisikaan käytännössä toteutettavissa sellaisinaan, niin selvityksen tekeminen paljasti monia huomioonotettavia asioita.

Henkilökohtaisesti koin saavani runsaasti tietotaitoa, ja osaaminen käsitellyistä aiheista kehittyi jatkuvasti työn aikana. Toivon pystyväni käyttämään osaamistani hyödyksi myös tulevaisuudessa IT-alan työtehtävissä, sillä tietosuoja-asetuksen seuraukset koskevat lähes kaikkia yrityksiä, jotka ovat tiedonsäilytyksen kanssa tekemisissä.

LÄHTEET

Andreasson, A; Koivosto, J & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma Oy.

Euroopan parlamentin ja neuvoston asetus 2016/679. Annettu 27.4.2016. Saatavilla sähköisesti http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY. Annettu 24.10,1995. Saatavilla sähköisesti osoitteessa http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:31995L0046

Hakala, M; Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Henkilötietolaki 523/1999. Annettu Helsingissä 1.6.1999. Saatavilla sähköisesti osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Koskinen, S; Alapuranen, L; Heino, A-J & Salli, M. 2005. Henkilötietojen käsittely työelämässä. Helsinki: Edita.

Kuikka, M. 2016. Tietojenkäsittelyn tutkimusmenetelmät, yhteenveto. Turun Ammattikorkeakoulu. Viitattu 10.4.2017. https://optima.turkuamk.fi/learning/id19/bin/user?nws=108636

Omnipartners.fi 2017. Poc eli Proof of Concept. Viitattu 4.5.2017. https://omnipartners.fi/sanakirja/poc-eli-proof-of-concept/

Opitietosuojaa.fi 2016. Yleistä tietosuojasta. Viitattu 17.1.2017 https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja

OTRS 5, 2015. OTRS database diagram. Viitattu 5.5.2017. https://raw.githubusercontent.com/OTRS/otrs/7a6cab39e8bacbadb2c89d304d24ad7747e17c6b/development/diagrams/Database/OTRSDatabaseDiagram.png

OTRS 5. 2015. OTRS Group.

Paavola, J & Vainikka, E. 2013. Näkökulmia Tietoturvaan. Turku: Turun Ammattikorkeakoulu.

Rope, T & Pöllänen, J. 1994. Asiakastyytyväisyys johtaminen. Helsinki: WSOY.

Tarhonen, M. Henkilötietojen pseudonymisointi – ai siis mikä? Sanoma. Viitattu 4.5.2017. https://www.iab.fi/iablogi/henkilotietojen-pseudonymisointi-ai-siis-mika.html

Tietosuojavaltuutetun toimisto 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen. Oikeusministeriö. Viitattu 10.4.2017. http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2017/01/uusiopasauttaarekisterinpitajiaeuntietosuoja-asetukseenvalmistautumisessa.html